e-LAWTREND

№ 1

January - April 2013

FREEDOM OF INTERNET IN BELARUS

THE REVIEW OF LEGISLATION AND PRACTICE

LEGAL TRANSFORMATION CENTER
220053 Belarus, Minsk, 38 Novovilenskaya Street +375 17 335 44 86 info@lawtrend.org
www.lawtrend.org www.fb.com/lawtrend

ASSESSMENT OF THE DRAFT NEW VERSION OF THE INFORMATION, INFORMATIZATION AND INFORMATION PROTECTION LAW * : CORRECTION OF ERRORS?

As it became known in early 2013, the House of Representatives of the National Assembly (i.e. Belarusian Parliament) is currently working on a bill whereby to amend the Information, Informatization and Information Protection Law ("the Bill"). The text of the Bill is available to the public and can be accessed on the National Law Portal of the Republic of Belarus (www.pravo.by).

The Information, Informatization and Information Protection Law regulates spheres that are critical for an information-based society: access to information, including socially important information under control of the state, and the protection of information (state secrets and other types of secret including personal data).

Why did the Law adopted relatively short time ago, in 2008, require such expedite revision? Will the proposed amendments remove gaps and flaws in the existing legal framework? Are the proposed amendments essential? Will they improve access to information about the activity of state agencies and the latter's transparency? Will personal data of individuals be protected?

Lawtrend experts have analyzed the publicly available Bill to grasp the idea of the direction and volume of the proposed amendments.

Scope of Regulation

It should be noted that the Law aims to regulate a wide range of social relations that occur in the information sphere in connection with the retrieval, receipt, use, transmission, collection, processing, accumulation, storage, distribution and provision of information. With the development of diverse e-government services and commercial online services, people increasingly often enter into various information-based relations, e.g. by filling in online forms and, thus, giving their personal data when making a purchase, searching and collecting information about potential customers, sending inquries/requests to state agencies in order to receive information under control of the state. In all of these cases people, in one way or another, get in contact with information, which means they fall within the scope of the Law.

To this end, it is of key importance for the state to ensure proper mechanisms to exercise two critical information-related constitutional rights: **the right of access to information** (Article 34 of the Constitution) and **the right to privacy** (Article 28 of the Constitution). They both belong to the fundamental human rights and are enshrined in the basic globally accepted documents (Article 12 and Article 19 of the Universal Declaration of Human Rights and Article 17 and Article 19 of the International Covenant on Civil and Political Rights).

The Law is intended to provide for the exercise of the said constitutional rights: the right to information is expressly specified in Article 6 of the Law and the right to privacy is implemented through the principle of protecting any individual's private life and personal data as one of the principles of law governing information-based relations (Article 4) and regulating legal protection of personal data (Article 18).

These are the above-mentioned critical information-related constitutional rights which require a closer public look to the Law and deeper scrutiny of the proposed amendments.

Current Version

It comes as no surprise that the Law adopted in 2008 has required expedite revision: the rapid development of information and communication technologies dictates adaptation of legal approaches to the new, "digital" conditions.

Moreover, significant flaws were detected

*** as at 30 April 2013.**

in the existing version of the Law. Lawtrend experts have already addressed the scope of the Law. Several gaps and deficiencies have been noted in the Belarusian legal framework governing the opportunities to exercise the right to privacy and the provision of the right of access to information.

In particular, it seems questionable to incorporate issues of both access to information and personal data protection into one law. The Law lacks a clear-cut definition for information belonging to the sphere of privacy and the same for personal data and fails to identify especially sensitive categories of information, e.g. medical data, therefore failing to provide for their adequate protection. It also deserves criticism that Belarus ignores international standards and best practices for the protection of automatically processed personal data and, in particular, demonstrates reluctance to implement the standards of the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data. At present, it is impossible for Belarus to formally accede to the Convention as Belarus is not a member of the Council of Europe.

In view of the above, Lawtrend experts arrive at the conclusion that the current version of the Law does need improvement and removal of deficiencies. The ensuing question is: will the newly proposed version remove these deficiencies?

Assessment of the Newly Proposed Version of the Law

It should be noted that this review only addresses the Bill which is made available for the public access and is currently under revision by the National Assembly House of Representatives, as the latter's official website reports. As the Bill has not yet been put on the Parliament's spring session agenda, the final version of the Bill may possibly include further corrections. Hence, this assessment also aims to evaluate the direction of the work over the newly proposed version of the Law.

The Bill proposes a relatively small amount of amendments to be introduced. In general, it preserves the overall structure of the existing Law and provides for insignificant modifications of Articles 12, 16, 17, 18, 24, 26 and 32, and more essential changes to Articles 21 and 22. The Law will include new articles, 181, 221 and 222.

It has to be pointed out that, seeking to improve the information-related legal framework, the Belarusian legislator refused to follow the path of adopting a separate personal data protection law and a separate one to regulate access to information. The Russian Federation, for instance, chose to draw a division between personal data protection and access to information and adopted two separate information-related laws, the Personal Data Law and the Law on the Provision of Access to Information about the Activity of State Bodies and Bodies of Local Self-Government. These changes in the legal framework enabled the Russian legal practice to make a significant move forward in the exercise of the information-related rights.

Right of Access to Information

The opportunity to send an electronic request for publicly accessible information is for the first time instituted at the overall legislative level (Article 21). It can hardly be viewed as a serious novelty rather than a streamlining attempt: at a narrower level, such an opportunity has been enshrined in the Law on Applications from Individuals and Legal Entities.

Information for Restricted Use and Distribution

While the list of publicly accessible information remains unchanged, the information for restricted use and distribution, i.e. the availability and/or dissemination of which may be limited, includes new categories.

1

A new article is added to the Law, Article 181, which deals with this type of information and defines the information for restricted use and distribution as “data related to the activity of a state body or other legal entity which, if disseminated and/or made available, may compromise national security of the Republic of Belarus, public order, morality, rights, freedoms and lawful interests of individuals including their honour and dignity, privacy and family life as well as rights and lawful interests of legal entities, and which do not belong to state secrets.”

Lists of data to be regarded as the information for restricted use and distribution will be formed at the discretion of heads of a state bodies or legal entities.

Additional Grounds to Refuse to Provide Information

2

Article 21 includes new reasons whereon requests for information may be rejected. For example, requested publicly accessible information may be refused to be provided if:

- the request implies the necessity to express a legal position on the request, analyze the activity of the state body or perform any other analytical work which is not directly connected with the protection of rights and lawful interests of the requester; and/or
- the requested information is published in official periodicals, mass media or placed for public access on Internet.

Notably, the Law does not oblige a state body to make any reference to such published information when rejecting a request.

In case “the requested information constitutes internal or office memoranda, instructions of officials and/or other internal correspondence of a state body or other legal entity as well as correspondence between state bodies and/or legal entities which are not directly connected with the protection of rights and lawful interests of the requester”, the request recipient may refuse to provide this information.

Access to Information on Official Websites

3

For the first time at the legislative level, the Bill sets up a norm allowing a state body to disseminate and/or make publicly accessible information available inter alia through publishing it on official websites of state bodies. The Bill stipulates that the Law will include provisions regarding the list of information which state bodies will be required to place on their websites.

An important novelty will be a norm requiring that those nation-level state authorities which are subordinate to the Government of the Republic of Belarus as well as local executive and administrative bodies publish annual reports (i.e. publicly accessible information about the results of their work) covering the preceding year and addressing main directions of their activity. Pursuant to the Bill, this information is to be published in the mass media and/or on websites no later than 1 March of the year following the reported one. It seems making more sense to establish the express obligation to place this information directly on the official website of a state body in question.

It should be noted that the above-mentioned list is based on the provisions of Presidential Order No. 60, Measures to Improve the Use of the National Segment of the Internet Network, and is added into the Law, almost word for word, from Council of Ministers Resolution No. 645, Certain Matters Regarding Websites of State Bodies and Organizations, which was adopted to implement the Presidential Order. This list neither introduces any new requirements to information to be published on official websites nor improve standards of access to information under control of state bodies.

Access to Open Meetings

4

Another new method of disseminating and/or making available publicly accessible information about the activity of state bodies, as provided by the Bill, is holding open meetings to be freely attended by individuals, their representatives and representatives of legal entities. Article 222 specifies that, unless issues containing information which is to be disseminated or made available on a limited basis are discussed, board meetings of nation-level state authorities subordinate to the Government of the Republic of Belarus and meetings of local executive and administrative bodies must be held openly.

A notice of the date, time and place of such open meeting and of its expected agenda must be published by state bodies on their websites and/or in the mass media and put at visible places on the premises of such state bodies, as a rule, no later than 5 calendar days prior to the date of such open meeting. The only access eligibility requirement to an individual or a representative of a legal entity is to bear a personal identity document, unless the respective state body arranged for prior registration to the open meeting. Subject to prior consent from the official presiding over the open meeting, attendees may take notes and/or photo, video and audio records.

Apparently, if adopted, these norms will become a significant step towards a greater informational transparency in the activity of the state and its bodies.

Personal Data Protection

Lawtrend experts would expect closer attention in the new draft version of the Law to such sector as the exercise of the right to privacy and the protection of personal data. First and foremost, it would be expedient to segregate personal data protection matters into a separate law (or at least into a separate chapter of the existing version of the Law) including the development of legislative terms and definitions in this sector and the normalization of the Law provisions with international standards, first of all, such as the standards of the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data.

Based on the assessment of the Bill, however, the new draft version of the Law, if adopted, will leave the problem of personal data protection virtually unresolved. To support this point, examples of privacy violations and leakage of personal data can be drawn. Regrettably, the legislator has currently been reluctant to go beyond a clarification that information related to an individual's private life and his/her personal data may only be collected, processed and stored upon his/her prior written consent (Article 18 of the Bill). No additional provisions to protect automatically processed personal data are planned in Belarus.

CONCLUSIONS AND RECOMMENDATIONS

In general, it should be noted that the amendments to the Law are relatively of cosmetic nature and will not solve any of the existing problems in this sphere of relations.

As mentioned above, Lawtrend experts are mostly disappointed by the lack of the legislator's attention to the yet unresolved problem of personal data protection and reluctance to follow approaches and principles set out in the Council of Europe legal framework as well as approaches of our immediate neighbours – Russian Federation and Ukraine. Notably, the absence of potent legislative regulation of the collection, storage, processing and transmission of personal data, first of all, lowers the legal status of ordinary individuals both in terms of the right to privacy to be observed and guaranteed and upon pursuing routine actions through Internet or electronic services, e.g. making purchases and ordering goods or services, receiving mails and sending inquiries/requests.

While noting positive changes to expand access to information by way of permitting attendance at open meetings of state bodies, one cannot but draw attention to the fact that the draft Law provides for loose terms of notification of the public about such open meetings, thus, relieving a state body in question of any responsibility for undue notification; also, the official presiding over such open meeting enjoys almost unlimited discretion as regards his/her permission to make notes/records. Similar excessive discretion is given to heads of state bodies/other legal entities when it comes to the provision of publicly accessible information as specified in Article 21.

Moreover, if a request for publicly accessible information is rejected, such a refusal does not require any reason to be given; no clear-cut criteria are specified for a refusal to either provide information or permit making notes/records at the open meeting. This may lead to a negative impact on the ways how this Law

will be applied, especially as far as problems of heightened public interest are concerned.

The introduction of the norm making it possible to disregard a request if it implies the necessity to state a legal position on the request, analyze the activity of the state body or perform any other analytical work which is not directly connected with the protection of rights and lawful interests of the requester generally seems to come into contradiction with the European practice which allows providing such information, e.g. to nongovernmental organizations acting in the interests of the general public (so-called social watchdogs). This norm may also narrow the ability of the public to influence socially important decision-making.

Although an obligation is going to be imposed on state bodies to upload certain information on their official websites, should this information be published in official periodicals, other mass media or other websites, a state body is not required to make any reference to such publications when rejecting a request for this information. This may give rise to information manipulations and, in certain situations, to perfunctory replies to information requests.

When evaluating the proposed version of the Law, one should bear in mind that much in this sphere in Belarus depends on the law-applying practice. To secure stronger safeguards for the rights and lawful interests of individuals and nongovernmental organizations, public oversight is essential both at the adoption phase of the Law and in further practice of its application. It can take such important forms as monitoring websites of state bodies, sending inquiries/requests to monitor information access compliance and public pressure to ensure further changes in the sphere of personal data protection.

5 LAW ENFORCEMENT REQUESTS FROM BELARUS FOR PERSONAL DATA ON 35 SKYPE ACCOUNTS / SKYPE USER SECURITY ISSUES

The Microsoft corporate blog has published the company's annual Law Enforcement Requests Report covering customer data disclosure requests it received in 2012.

The Microsoft Company notes that as outlined in its Global Human Rights Statement and in keeping with its commitments as a member of the Global Network Initiative, it recognizes the important responsibility it has to respect human rights and the principles of free expression and privacy. For that purpose, it regularly reviews and updates its relevant policies, processes and management systems. As part of its commitment to transparency, the company provides, on an annual basis, public access to the information on the criminal law enforcement requests it receives with regard to customer data. The data on law enforcement requests related to various Microsoft products are reported separately from the same for Skype due to different legal frameworks applied. Also, a different legal regime is applicable to handling law enforcement requests from the United States and Ireland either because the company is headquartered in those jurisdictions or because it hosts data in those countries. A similar legal regime applies to Skype with regard to law enforcement requests from Luxembourg.



Microsoft provides SSL encryption for Microsoft services, and Skype-to-Skype calls on the company's full client (for full-function computers) are encrypted on a peer-to-peer basis. However, it should be emphasized that no communication method is 100% secure. For example, Skype Out/In calls are routed through the existing telecommunications network for part of the call, and users of the Skype thin client (used on smartphones, tablets and other hand-held devices) route their communications over a wireless or mobile provider network where they might be controlled. In addition, the end points of a communication are vulnerable to access by third parties such as criminals or governments. Accordingly, all users are encouraged to exercise caution, take measures to prevent their computers and devices from being infected with malicious software, and obtain updates from known and trusted sources only.

The company points out that while it respects the fact that law enforcement entities have the very difficult job of providing safety and security and bringing to justice those who commit crimes, at the same time, it remains cognizant of the potential for law enforcement activities to infringe upon human rights and free expression. Each year the company receives and processes requests from many countries of the world. The company does not honor requests that do not follow its principles and policies as it understands that some users of Microsoft services may be subject to government monitoring or the suppression or control of ideas and speech.

According to the published report, Belarusian law enforcers forwarded five requests to the company concerning 35 Skype accounts in 2012. Responding, the company disclosed the so-called identifiers specified in the requests received. The correspondence itself or any other

data which comprise the content of correspondence or video/voice communications was not disclosed. Belarus appears only on the list of Skype-related law enforcement requests. No requests from Belarusian law enforcers were received on customer data related to users of other Microsoft products or services.

In dealing with law enforcement requests, Microsoft discloses customer data to law enforcement agencies only on the basis of valid court orders or similar legally binding and duly executed requests which Microsoft reasonably regards as authentic. Disclosure of information is limited to providing non-content data. In those cases where Microsoft does not have sufficient grounds to believe that law enforcement requests are connected with criminal investigations, the company rejects them and does not disclose any customer data.

This is how disclosed non-content data, i.e. containing no correspondence details or private information looks like:

Field	Value
Login	First.Last@xxxxxxx.com
PUID	0006BFFDA0FF8810
First Name	First
Last Name	Last
State	Washington
Zip	98052
Country	US
Timezone	America/Los_Angeles
Registered from IP	65.55.161.10
Date Registered {Pacific}	10/24/2007 1:05:18 PM
Gender	M
Age	1977
Last Login IP	64.4.1.11

When asked by Belarusian independent media, the Microsoft Company made the following comment on the law enforcement requests from Belarus: "The Microsoft Compliance Team thoroughly examined all the five requests from Belarusian judicial bodies which evidenced that law enforcement agencies were involved in criminal investigations into thefts via stolen credit cards. We would like once again to draw your attention to the fact that no information beyond non-content data and no information related to data exchange content was disclosed in any of the Skype-related cases."

At the same time, the issue of Skype security in terms of law enforcers' access to personal data of Skype users and their ability to obtain copies of messages and wiretap Skype calls was widely discussed in first quarter of 2013 in the Russian segment of Internet.

For instance, according to Vedomosti, a Russian newspaper, the general manager of Group-IB, a Russian company, reportedly insisted that intelligence agencies had been able, "for a couple of years already," to both wiretap and locate Skype users.

Extract from Microsoft's Law Enforcement Requests Report regarding Skype users:

Law Enforcement Requests Report

Skype

This data set is for Skype only.

	Calendar Year 2012			July 2012 - December 2012	
	Total # of Requests	Accounts/Identifiers Specified in Requests	Requests Resulting in Disclosure of Content	Accounts Specified in Requests Where Compliance Team Found No Data	Provided Guidance to Law Enforcement
TOTAL	4,713	15,409	0	2,847	501
Argentina	2	5	0	1	1
Armenia	2	6	0	3	0
Australia	195	424	0	118	8
Austria	10	18	0	0	4
Belarus	5	35	0	0	0
Belgium	39	165	0	45	3
Brazil	8	36	0	1	0

After Microsoft acquired Skype in May 2011, it equipped the Skype client with a lawful wiretapping technology, tells the Peak Systems CEO. Now any subscriber may be switched to a special mode where encryption keys which are normally generated in the subscriber's phone or PC will be generated by the server. By getting access to the server, it is possible to wiretap a conversation or read correspondence. Microsoft makes this technology available to law enforcers worldwide, including Russian ones, the expert explains. According to information security experts, Russian intelligence services obtain access to Skype correspondence and conversations not only under court orders – sometimes it happens "just by request." It's a misconception to believe that Skype wiretapping is an insoluble problem for Russian law enforcement agencies, confirms a police official. Official representatives of the Russian Ministry of Internal Affairs and Federal Security Service refused to comment. Earlier, Nikolai Pryanishnikov, head of Microsoft Russia, said that Microsoft might disclose the Skype source code to the Federal Security Service. In itself, the code would not allow intelligence services wiretapping conversations but could make it easier for them to find a proper "deciphering" solution.

As it's known, the Chinese version of Skype includes a special mechanism to monitor user actions. The Chinese Skype installation kit has a built-in key logger, a special application recording all user keyboard actions. It checks texts for unwanted words and sends collected logs to intelligence services. The list of unwanted words allegedly includes such words as Tiananmen (the square where the 1989 protests were suppressed), Human Rights Watch, Reporters without Borders, BBC News etc.

In the Belarusian judicial practice, Skype data were used against the 19 December 2010 protest participants. In particular, a Skype conversation by Sergey Martselev was used as evidence in the case against Statkevich, Uss, Pozniak, Klaskovskiy, Kviatkevich, Gribkov and Bulanov. The defence motion to summon Martselev before the court as a witness was rejected. Some other facts also make it possible to conclude that Belarusian intelligence services seek to get access to, and make use of, Skype customer data.

LIABILITY FOR BREACHING PRESIDENTIAL ORDER NO. 60: 5 ADMINISTRATIVE OFFENCE PROTOCOLS IN 2012

Presidential Order No. 60, Measures to Improve the Use of the National Segment of the Internet Network, became effective on 1 June 2010. It stipulates for liability in case of breaching its provisions, but the respective changes to the Belarusian Code of Administrative Offences (CAO) were made only in late 2011 and came into force on 5 September 2012. According to CAO Article 22.16, there are three elements of offence in this sphere:

1. Provision of goods, works or services in the territory of Belarus by using Internet-connected information networks, systems or resources which are not physically located in the territory of Belarus and/or duly registered;

2. Violation of requirements established by law prescribing to maintain identification of customer devices when providing Internet services and/or users of Internet services in public multi-access outlets, and record and store data about customer devices, Internet users' personal data as well as information about Internet services provided;

3. Violation of requirements established by law prescribing to restrict access for Internet services users to information which is prohibited by law from distribution.

Those liable of noncompliance are to be fined up to 30 Base Fee Units*.

At the same time, public access to the information about any facts of bringing to this liability with the indication of particular elements of offence under CAO Article 22.16 is limited as these data are not published.



However, it was in his interview to Euroradio, when **Vladimir Ryabovolov from the Operative Analytical Center**, for the first time disclosed data on the existing enforcement practice:

"*We reviewed the last year's administrative practice: only 5 administrative offence protocols were executed for breaching [Presidential] Order No. 60, and they were unrelated to Internet cafés. The protocols were mostly executed by tax authorities and were connected with providing goods, works or services through resources outside the national Internet segment. I'd like to say that many provisions of [Presidential] Order No. 60 are adopted to protect property rights of citizens. For instance, a person buys a poor-quality mobile phone and attempts to claim it but the seller's whereabouts are unknown. That's why a provision is set that goods, works or services may only be sold through resources located in the territory of Belarus. As the practice shows, violations are few. Whether it's good or bad? To me, it's good. Universally understandable rules were developed, and the system brought itself to discipline.*"

ABOUT THE ACTIVITY OF THE NATIONAL TRAFFIC EXCHANGE CENTER (NTEC)

Presidential Order No. 515 dated 30.09.2010, Certain Measures to Develop a Data Transmission Network in the Republic of Belarus, approved the establishment of a Common National Data Transmission Network (CNDTN) to incorporate data transmission networks of national government agencies, local authorities and other state bodies and organizations including economic entities whose decision-making may be controlled by the Republic of Belarus or its administrative/territorial units due to their interest/shares in the chartered capital. The CNDTN does not incorporate those data transmission networks which are designed to ensure national security, defence or public order.

To implement this Presidential Order, a national unitary company, the National Traffic Exchange Center (NTEC), had been established by 1 December 2010. By law, NTEC is entitled to perform the following functions:

- to ensure protection from unauthorized access to CNDTN and data transmitted through it, gate the traffic and manage CNDTN and provide for its development;
- to ensure interface between data transmission networks and interaction between state bodies and organizations and other legal entities and individual entrepreneurs in the provision of telecommunication services via CNDTN;
- to ensure equal access opportunities to CNDTN for state bodies and organizations and other legal entities and individual entrepreneurs;
- to arrange settlements for the connection of data transmission networks to CNDTN and services provided through CNDTN (including the approval of pricelists and rates);
- to exert technical control over the gating of international traffic and the connection to foreign telecommunication networks;
- to set up data processing centers, information networks/systems/resources and points of connection to foreign telecommunication networks and ensure their proper operation.

Data transmission networks of state bodies and organizations and other legal entities and individual entrepreneurs are connected to CNDTN via NTEC following the procedure described in the Regulations for the Common National Data Transmission Network (approved by joint Resolution No. 8/28 dated 27.12.2010 adopted by the Operative Analytical Center under the President of the Republic of Belarus and the Ministry of Communication and Informatization of the Republic of Belarus).

Notably, NTEC and Beltelecom are the only telecom operators authorized to gate international traffic and get connected to foreign telecommunication networks, which is often reasonably viewed as the state monopoly in the sphere of gating and selling traffic to national Internet services operators.

Vladimir Ryabovolov, an OAC representative, expressed his view of NTEC activity and its impact on the removal of Beltelecom's monopoly:

«In my OSCE address, I said that there are a number of factors deterring the development of the IT sphere in Belarus. One of them is the de facto monopoly of Beltelecom. To say the only one would not be the case. Many positive things are associated with Beltelecom. Historically, it's our largest nationwide telecom operator. Many things implemented in Belarus are done due to Beltelecom's participation. A major part of the network, approximately 80 per cent, is in Beltelecom's ownership. It de facto owns the external gate; all the traffic gets through it, and it further sells it to the others. Any price parity failed to be achieved. Perhaps, it's a problem to a certain extent. We studied [the existing] world practice. The reforming of national telecoms was effected in many countries of Central and Eastern Europe. We aren't the first here – it's an established practice. I assume the creation of normal competitive environment will be a condition to improve efficiency of all market stakeholders, including Beltelecom. The creation of NTEC gave birth to certain expectations. The information environment is already there, that's why competition has started to materialize. Also, some moves on Beltelecom's end were felt resulting in the price drop. So far, NTEC has not yet reached its full function. A number of tasks are to be performed for that: first of all, to create infrastructure, then to provide technical equipment and, of most importance, to ensure significant investment. To that end, Belarusian Cloud Technologies, a company co-owned by NTEC, has been established. We'll soon feel a real output of its activity. Authorizing NTEC to operate as a national telecom is the first step. This process will be continued. Perhaps, real competition implies a large number of [competing] entities. We should responsibly approach to what has already been created in our country. Beltelecom is, nevertheless, a large-scale organization. It a social issue: it has over 20 thousand employees, an established team, traditions… Creating something new, we should take into account those good things that have been done before us».

WEBSITE BLACK LISTS: HOW DOES IT WORK?

Restriction of access to certain websites was introduced by Presidential Order No. 60 dated 01.02.2010, Measures to Improve the Use of the National Segment of the Internet Network.

As a result, Internet services providers shall restrict access

a) for state agencies and organizations and health care, education and culture institutions and

b) upon request, for other users of Internet services to any information encouraging:

- extremist activity;
- illegal circulation of arms, ammunition, explosive assemblies, explosive, radioactive, poisonous, potent, venomous and toxic substances, narcotic drugs, psychotropic agents, their precursors and similar substances;
- assistance in illegal migration and human trafficking;
- distribution of pornographic items;
- promotion of violence, cruelty and other acts prohibited by law.

Specific restriction procedures are enacted by joint Resolution No. 4/11 dated 29.06.2010 adopted by the Operative Analytical Center (OAC) under the President of the Republic of Belarus and the Ministry of Communication and Informatization of the Republic of Belarus. It sets forth the Regulations for the Procedures to Restrict Access for Internet Services Users to Information Prohibited by Law from Distribution. Internet services providers are to ensure the restriction of access pursuant both to the Restricted Access List maintained by the State Telecommunication Inspectorate of the Republic of Belarus (BelGIE) under the Ministry of Communication and Informatization and their own access restriction lists.

BelGIE forms its Restricted Access List on the basis of decisions taken by heads of the State Control Committee, Office of the General Prosecutor, OAC and national government agencies (hereinafter referred to as “authorized state bodies”) to include Internet resource identifiers on the Restricted Access List. Such decisions by heads of authorized state bodies must fall within their scope of competence.

Within 3 working days following the decision date authorized state bodies duly notify of it:

- BelGIE; and
- the holder/owner of the Internet resource which is restricted from access provided that it is part of the national Internet segment.

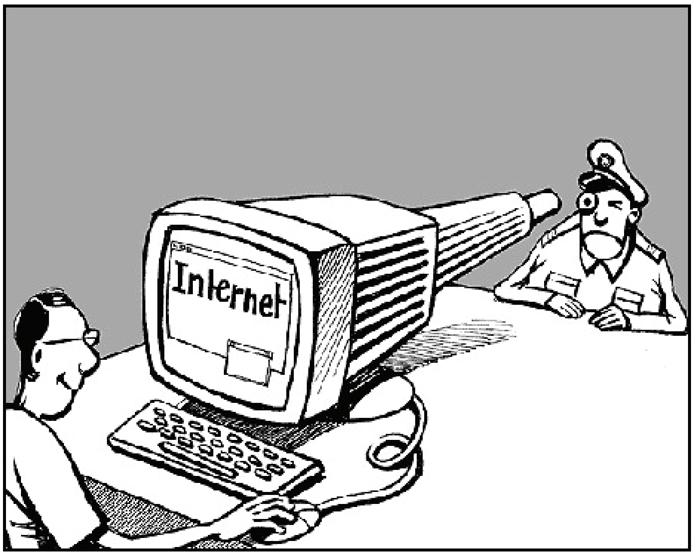
The notice includes:

- identifiers of the Internet resource subject to restricted access;
- reasons for the restriction of access with reference to the respective law provision(s) prohibiting this type of information from distribution

In case the reasons for keeping identifiers of an Internet resource on the Restricted Access List cease to exist, the authorized state body which took the decision on the inclusion decides to exclude the Internet resource identifiers from the restricted Access List. Within 3 working days the authorized state body duly notifies of the decision BelGIE and the holder/owner of the Internet resource which is restricted from access provided that it is part of the national Internet segment.

Legal entities, their branches and representative offices, individual entrepreneurs and physical persons have the right to apply to authorized state bodies and make proposals regarding the Restricted Access List.

The Restricted Access List is published on BelGIE website. It can be accessed at http://belgie.by/node/216. Actually, there are two Restricted Access Lists: one for public use (in fact, it's an empty Excel file offered for download when you click on the link) and the second one for Internet providers which is restricted from access by ordinary users (needs an Internet provider's login and password).



The data included in the Restricted Access List with identifiers of Internet resources registered in the national Internet segment are for public use. Actions of authorized state bodies related to the formation of the Restricted Access List may be challenged in court.

Regarding the "black lists" of websites, the OAC representative **V. Ryabovolov**, in his public interview, explained the following:

> *«The inclusion procedure is laid down in detail. BelGIE is assigned to maintain the lists; it forms them on the basis of substantiated conclusions by authorized state bodies. To the best of my knowledge, most of these sites contain porno materials and pages of extremist nature. To my information, 119 resources in total are included. Why cannot be accessed publicly? Should they be in public access, this would induce additional interest to them. Why making promotion to them? Moreover, they are restricted from access by state bodies and educational institutions only. As for the inclusion, affected persons may apply to BelGIE; the appellation is an admissible mechanism – there must be a possibility to appeal. One of the speakers at the OSCE Conference plenary meeting said: it should be transparent, substantiated and give the right to appeal. Our procedure is transparent, the inclusion is substantiated and there's the right to appeal».*

WITHDRAWAL OF MANDATORY PASSPORT-BASED IDENTIFICATION OF INTERNET CAFE USERS



On 22 December 2012, amendments were adopted to the Regulations for the Operation of Computer Clubs and Internet Cafes (approved by Council of Ministers Resolution No. 175 dated 10.02.2007). **As a result, data transmission services or telematic services may now be provided to individual users upon his/her identification through one of the following options:**

To select (a) particular identification method(s) is up to the managers of computer clubs or Internet cafes or person authorized by them.

According to OAC, not all Internet cafés and computer clubs were happy about this innovation, because installing additional equipment means additional expenses. At the same time, as mentioned above, it's up to cafes or clubs, not users to decide which permitted identification option to select from the above list.

When the amendments came into force, Euroradio journalists checked the situation in Internet cafés and public access outlets in Minsk. The innovations notwithstanding, nothing had actually changed: passport-based identification was still the only option; in some cases administrators agreed to accept other IDs, such as driving licences or library tickets. Although admissible by law, photo, video or SMS user identification is out of practice yet.

- a personal identity document to be produced by the user;
- other means enabling to establish his/her identity (personal club member card, access card or similar);
- technical means enabling photo/video recording;
- other software and hardware methods (including SMS) enabling to compare users' network details with their personal data.

E-GOVERNMENT IN BELARUS

In March 2013, a delegation from South Korea visited Minsk to discuss the establishment and operation of the so-called electronic government. The delegation met with a number of officials, including Vsevolod Yanchevskiy, a presidential aid. The Ministry of Communication explained the reasons why namely South Korea was chosen for cooperation in this sphere: the country has been topping the respective UN list of 193 countries for 2 years in a row, and Koreans allow themselves teaching others and transfer positive experience.



However, **Dmitriy Gavrusik**, an e-gov.by expert, is of a slightly different opinion: the Korean e-government model is close to our officials' perceptions and expectations. Koreans apply a centralized approach where it is the government who sets priorities, works out a program and implements it. In a centralized approach, the government is responsible for funding the project as it requires quite a huge portion of investment. An opposite example is Estonia where private companies are involved in the process, including its financial component. Businesses take part in the creation of the e-government and profit on it afterwards. As for Belarus, Br11,000,000,000 is allocated for the establishment and operation of the electronic government.





According to **Mikhail Doroshevich**, e-Belarus.org project leader, studying world experience, including the Korean one, is reasonable but optimal solutions should be tailored specifically for Belarus.

High ranks in the UN e-government establishment and operation list also belong to the Netherlands, UK, U.S., Denmark, France, Norway, Greece and Finland.

Belarus has around 100 available e-services, an infrastructure, information resources of state authorities and an e-services center. At the same time, Dmitriy Gavrusik notes, all this lacks a focus on consumers, i.e. individual citizens. As no information about the services is disseminated, very few consumers know which services are now available, and a number of links on the government services portal does not work.

The European Commission requires at least 25 services to be accessible by citizens via Internet. At the same time, simply replicating these services does not make an e-government. Among positive aspects in Belarus, it is noted that state cadastres, registers, auctions and tenders are open for public access via Internet.

AMERICAN INTERNET ACTIVIST DIES FOR WEB FREEDOM



One of the world's most prominent Internet activists advocating the freedom of information, Aaron Swartz, committed suicide in January 2013 in New York.

Born in 1986, he became a co-author of the RSS 1.0 specification at the age of 14, wrote a number of books formulating an IT-space philosophy, in particular Who Writes Wikipedia and HOWTO: Be More Productive, created a web service, Infogami, which later merged with a popular website Reddit, and also co-founded an organization against Internet censorship, Demand Progress. When working for the Harvard University Center for Ethics in the 2010-2011 academic year, he wrote a political corruption research paper and later launched a dedicated website, watchdog.net, which addresses the same problem. Swartz also worked on another special nonprofit online project, Open Library, intended by its creators to collect and store "every book ever published" in electronic format.

The reason for the activist's suicide was criminal charges brought against him by Massachusetts state prosecutors and the administration of the Massachusetts Institute of Technology (MIT). Accused of fraud, Swartz did not plead guilty. The trial was scheduled for April 2013. Based on the 13-item charges against him (violation of peering rules, computer fraud and illegal download of content from a protected computer etc.), Swartz faced up to a total of 35 years in prison.

The official charges insisted that he had allegedly stolen materials from the online service JSTOR which offered pay access to publications from scientific journals. The prosecution alleged that the hacker had intended to upload them to one of free file sharing networks. The online service JSTOR offers free guest access to staff members of certain scientific institutions and Swartz, as an employee of the Harvard University's Safra Center for Ethics, had the right to such access. JSTOR refrained from any legal action against Swartz.

Swartz's defence position was the following:

Swartz enters the campus's computer network which does not limit third-party connections at all, gets connected to the article archive service which is also unrestricted and accessible to the network users and, having written a number of simple scripts, downloads several gigabytes of information. That is, he does not break into a closed network, does not attempt to get access to any restricted data – he just downloads more than he needs at this particular point of time to provide further access for a broader segment of the public to scientific publications paid by taxpayers' money but unavailable to the overwhelming majority of those who paid for them.

However, as Swartz committed suicide, no trial will ever happen. In protest against the prosecutors' actions and in memory of Aaron Swartz, a large-scale campaign started in the Internet. Scientists from all over the world publish links in Facebook and Twitter to copyrighted scientific documents, and JSTOR announced that it would soon upload for free access about 4.5 million files. Hackers from Anonymous attacked the website of the Massachusetts Institute of Technology and placed there an obituary to Aaron Swartz. They also attacked the website of the United States Sentencing Commission, an independent agency of the US federal government, which is responsible for articulating the sentencing guidelines to be used by American federal courts.

Aaron Swartz's death will have far-reaching implications. The existing copyright system is increasingly becoming a subject of much discontent, and the necessity to review and re-comprehend the right to copy and distribute information is getting increasingly obvious day by day: it is unjust to follow unjust laws. Reacting to the sorrowful event on its website, the Electronic Frontier Foundation, an organization advocating free distribution of information, called Swartz "an extraordinary hacker and activist," adding that he "did more than almost anyone to make the Internet a thriving ecosystem for open knowledge, and to keep it that way."